United Nations A/CONF.213/IE/4

Twelfth United Nations Congress on Crime Prevention and Criminal Justice

Salvador, Brazil, 12-19 April 2010

Distr.: General
19 March 2010

Original: English

Items 8 of the provisional agenda*

Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime

Background documents** received from individual experts***

EXTRADITION & CYBERSPACE

Prepared by

Henrik S. Spang-Hanssen

* A/CONF.213/1.

** Distribution is limited to the quantities and languages in which the paper is made available to the United Nations Office on Drugs and Crime.

*** The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

EXTRADITION & CYBERSPACE

Presented to
The Twelfth UN Congress on
Crime Prevention of and Criminal Justice
Salvador, Brazil, 12-10 April 2010

by
Henrik S Spang-Hanssen,[1] *Independent Senior Researcher*
(formerly Prosecutor and Supreme Court Attorney-at-law in Denmark)

Silicon Valley, California, USA
hssph@yahoo.com
http://hssph.net

---

1. Introduction

Today's children and adults use computers. Children use computers to learn, experiment and play. Adults use computers in many aspects of life - for example, communication with friends and government, exchange of opinions, and online banking. At least adults can be expected to know the law of their own country.

However, some use of computers can also - unknowingly - imply/mean violation of foreign laws. This is to a large degree due to an unsolved matter in public international law related to Cyberspace - the jurisdictional question, that is, where is the (relevant) place(s) where things happens when a person use a computer connected to the Internet and thus which law(s) apply [see further my additional paper on the jurisdictional issue]. The only existing treaty[2] relating to Cyberspace[3] makes no suggestions to this vital issue.

---

[1] Author of among other things: **The Future of International Law: CyberCrime** (2007)(available from the Social Science Research Network's (SSRN's) Working Paper Series at http://ssrn.com/abstract=1090876); **A Just World under Public International Law in Cyberspace: Jurisdiction** - Chapter 1 to: "CYBER JURISPRUDENCE" (Icfai University Press, 2008); **Cybercrime Jurisdiction in Denmark** - Chapter 8 to: CYBERCRIME JURISDICTION: A GLOBAL SURVEY (T.M.C. Asser Press , 2006); **Public International Computer Network Law Issues** (Chapter 7 on cyber crime)(DJØF Publishing, 2006); **Cyberspace & International Law on Jurisdiction** (DJØF Publishing, 2004).

[2] The (European) CyberCrime Convention of 2001 (or "Budapest Convention "), ETS no. 185 of 23 November 2003 (entered into force 1 July 2004) at http://conventions.coe.int/treaty/en/treaties/html/185.htm. Chart of signatures and ratifications, Council of Europe at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=10/03/2010&CL=ENG (last visited 9 March 2010).

As most acts done on the Internet involve cross-border transmissions, the effects of a citizen's computer use can be felt both domestically and in a foreign country. This implies that not only national law but also foreign law is involved. Thus, international cooperation is needed.[4]

Furthermore, it means that today – because of the extreme, and still increasing, number of computer users and because of cross-border transmissions involving foreign law – the issue of extradition has become very significant, central and a frequent occurrence.

The coming decade will without doubt show an escalation of numbers of citizens required to be extradited because of the effects of their computer use having been felt in foreign countries.

The following section will provide some scenarios, which are the sum of many situations that have occurred in the past or will occur. I have used a child-based scenario in part. But to a large extent it also applies to the adult environment, because it has often been the case that children are more advanced computer users than their parents and other adults.

2. Scenarios

Ahmed, a 15-year-old, is somewhat of a computer nerd. He invents a software program that should be able to retrieve forgotten passwords. He tests the software on his own and his father's computers and it seems to work.

Ahmed tells one of his co-workers at a supermarket, Enrico – who is over 18 – about the software. Enrico copies the software from Ahmed's laptop while it is unattended. Enrico likes to hack into computers just to find out whether he can bypass firewalls, etc. He uses Ahmed's software to hack into foreign state CDONU's military computer network. Enrico never intends to destroy or copy anything. However, in this instance he cracks some parts of the CDONU military's systems, due to an unintended feature in Ahmed's software.

The CDONU military notifies the police about the break-in. The police discover that Enrico has copied Ahmed's program and require that Enrico and Ahmed be extradited for prosecution.

Meanwhile, Louise, an 18-year-old, writes an essay on religion as a school-assignment. She uploads the paper on a website, which only uses the language of her country.

A clergyman on a foreign continent discovers Louise's paper on the website. He is able to read the foreign language, is appalled about the content, and calls for his local law enforcement agency to bring criminal charges against Louise.

Both Louise's and the clergyman's countries are parties to the CyberCrime Convention of 2001,[5] which requires each party to prosecute or extradite violators. Neither Ahmed's nor Enrico's country is a party to this convention.

Elsewhere, a woman belonging to a criminal gang approaches a 14 years old girl, Tania, in a public library and asks her whether she wants to earn $100 by connecting a USB flash-drive stick to one of the public library's computers and pressing an "OK" button when it appears on the screen. The woman explains that she is not personally confident in using computers.

Tania accepts the offer, inserts the USB stick, and clicks "OK" on the screen, which next states that "all is well and the program will now shut down itself." What actually happens is that the clicking

---

[3] In 2000, scholars at Stanford University drafted "A Proposal for an International Convention on Cyber Crime and Terrorism" (Draft by George D. Wilson, Abraham D. Sofaer and Gregory D. Grove, Center for International Security and Cooperation (CISAC), Hoover Institution) at http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf (last visited 9 March 2010), reprinted in THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 58 (A. Sofaer and S. Goodman, eds., Hoover Institution Press 2001 – ISBN 0-8179-9982-5). Also available from http://www.hoover.org/publications/books/cybercrime.html (last visited 9 March 2010).

[4] In matters of international cooperation, criminal justice agencies must rely, to a large extent, on the treaty network developed by their country. To facilitate international cooperation in criminal matters, the UN General Assembly adopted a Model Treaty on Mutual Assistance in Criminal Matters www.unodc.org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf (last visited 10 March 2010)). Strengthening the convergence of criminal law and criminal law procedure is also part of any long-term strategy to build more effective international cooperation.

[5] The (European) CyberCrime Convention of 2001 (or "Budapest Convention ") - ETS no. 185 of 23 November 2003 (entered into force 1 July 2004) at http://conventions.coe.int/treaty/en/treaties/html/185.htm. Chart of signatures and ratifications, Council of Europe at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=10/03/2010&CL=ENG (last visited 9 March 2010). See also "A Proposal for an International Convention on Cyber Crime and Terrorism" (Draft by George D. Wilson, Abraham D. Sofaer and Gregory D. Grove, Center for International Security and Cooperation (CISAC), Hoover Institution) at http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf (last visited 9 March 2010), reprinted in THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 58 (A. Sofaer and S. Goodman, eds., Hoover Institution Press 2001 – ISBN 0-8179-9982-5). Also available from http://www.hoover.org/publications/books/cybercrime.html (last visited 9 March 2010).

the OK button initiates a program that starts copying several stores' credit card data, which is then transmitted to the criminal gang's computer in foreign country Charge. Tania's country is not a party to the CyberCrime Convention.

Ahmed's government rejects the request it has received to extradite him to the foreign country CDONU as he has not violated any national law in his own country and is a minor.

Enrico has not violated any national law in his own country. The foreign country CDONU nevertheless demands his extradition for having violated its criminal code on national security. Enrico's attorney brings the government's decision to extradite him before the courts. On appeal, the supreme court decides to allow the extradition. However, the court adds conditions to the extradition, namely that any jail sentence imposed cannot exceed the maximum limit for similar national security codes in Enrico's country (twenty years) and, further, that the sentence has to be handed down in total for all the offenses found by the court in CDONU.

A jury in CDONU finds Enrico guilty of three charges, which verdict would normally carry a sentence of three times sixty (i.e., 180) years in jail pursuant to CDONU criminal code, with a right to parole after two-thirds of the time is served. However, the court in CDONU reduces the jury's sentence to twenty years due to the extradition conditions attached by Enrico's country.

As for the article on the website, Louise's work is protected by her state's constitutional's free-speech provision. Louise's government decides not to prosecute the claim from the clergyman's country. But due to the CyberCrime Convention's mandatory rule of "prosecute or extradite," the government determines it must extradite Louise. Nonetheless, on appeal, the country's supreme court rules in favor of Louise's claim against extradition based on the protection in the constitution.

Tania's local police find she did not have had any intent to violate any law and determine not to press any charges. However, country Charge requires Tania to be extradited and her country's government authorizes extradition due to an existing bilateral extradition-treaty. A jury in country Charge then finds Tania has violated its criminal code pursuant to which it is a crime to copy credit card information from a database. The code has a "Three Strikes Rule," under which the minimum sentence of imprisonment is 25 years. The jury finds seven databases have been copied and that the Three Strikes Rule should be used. Tania is sentenced to 25 years in prison.

3. Comments

The above scenarios illustrate how easy it is for acts done on computers to become foreign crimes. Thus, the question of extradition also comes into play.

Extradition has traditionally not been that much of an issue. Yet with the invention of the personal computer, and the widespread network connections established via the Internet, the issue has grown in significance. There would seem to be no doubt that an escalation in the numbers of citizens required to be extradited will occur because of the effects of their computer use being felt in foreign countries. The increasing number of news articles on the subject bears this out – and shows that public interest in the matter is also growing.[6]

Accordingly, countries need to continue to develop and refine their treaty network and to modernize their extradition treaties. The often cumbersome processes of extradition need to be streamlined.[7]

---

[6] See for example the worldwide coverage of the McKinnon case (extradition of an English citizen to the US). Self-confessed hacker Gary McKinnon hacked into 97 US federal and military computer systems, and was accused of trying to get into 73,000 others. The US claims McKinnon's exploits, between 2001 and 2002, are the greatest military hack of all time and caused damage worth at least £350,000. However, the UK National High Tech Crime Unit found no evidence on McKinnon's computer that he had damaged US systems. On 28 August 2008, the European Court of Human Rights decided to refuse Gary McKinnon's request (no. 36004/08) for interim measures and such that the Court would not prevent his extradition from the United Kingdom to the United States. See the court-resume at http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=839381&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649 (last visited 11 March 2010). On 4 July 2006, the UK Secretary of State decided that McKinnon should be extradited. See also Gary McKinnon v. Secretary of State for the Home Affairs, [2007] EWHC 762 (Admin)(UK High Court, Queen's Bench, 3 April 2007) (appeal dismissed), [2008] UKHL 59 (UK HL, 30 July 2008)(appeal dismissed), [2009] EWHC 170 (Admin)(UK High Court, Queen's Bench, 23 January 2009)(Hearing), [2009] EWHC 2021 (Admin)(UK High Court, Queen's Bench, 31 July 2009)(review denied).

[7] The existing regime of international cooperation in criminal matters is still in need of major improvements to avoid legislative loopholes and to eliminate safe havens. See pages 8-10 in Criminal Justice Assessment Toolkit: Cross-Cutting Issues # 4 -

For such purpose, the United Nations Model Treaty on Extradition has been drawn up.[8] Furthermore, the UN Conventions against Transnational Organized Crime and against Corruption[9] address some of the extradition issues that have arisen and recommend means to simplify evidentiary requirements and keep the burden of proof to a minimum in extradition proceedings. These conventions set basic minimum standards for extradition for offenses they cover and also encourage the adoption of a variety of mechanisms designed to streamline the extradition process.

The coming decade should show increased numbers of people required to be extradited given the effects of their computer use in foreign countries.

Thus, the international community arguably needs to address the question of computers and the obligation to extradite or prosecute (aut dedere aut judicare) soon. The UN General Assembly , in paragraph 5 of its resolution 60/22 of 23 November 2005, endorsed the decision of the International Law Commission to include the topic "The obligation to extradite or prosecute (aut dedere aut judicare)" in its long-term programme of work.[10] The Commission has most recently discussed the issue in 2009.[11]

So far, however, the UN International Law Commission has not dealt specifically with the issue of computers/Internet and extradition. And, ultimately, it is the domestic law of the requested States that governs how extradition works.[12]

As a result, as demonstrated in the above scenarios, different countries will deal in their own ways with criminal violations committed by their citizens' use of computers.

In many cases, the violators – whether minors or adults – will have no idea about which countries in which they can be indicted or about how they may be tried, convicted, sentenced and imprisoned. There is no predictability, because the international community has not yet resolved where, that is in which state, computer-related criminal acts are initiated, done and executed – and where there is jurisdiction to adjudicate them.

Bilateral treaties on extradition are too numerous to keep track of nowadays.[13] This fact, of course, makes it impossible for an individual cybernaut to be aware of, or have even the faintest idea about the law with which they must comply.

Furthermore, to date, many courts in different countries – when confronted with computer/Internet crimes – have exercised what could be called "Global Jurisdiction"[14] – not to be

---

International Cooperation (UNODC, 2006) at http://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/4_International_Cooperation.pdf (last visited 10 March 2010).

[8] See http://www.unodc.org/pdf/model_treaty_extradition.pdf (last visited 10 March 2010). Extraditable offences are offences that are punishable under the laws of both Parties by imprisonment or other deprivation of liberty for a maximum period of at least [one/two] year(s), or by a more severe penalty - death penalty is not accepted.

[9] Article 16, see http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf (last visited 10 march 2010).

[10] Page 221 in Chapter IX on "The obligation to extradite or prosecute (aut dedere aut judicare)" of the Report of the International Law Commission, Fifty-ninth session (June-August 2007), General Assembly Official Records, Supplement No. 10 (A/62/10) at http://untreaty.un.org/ilc/reports/2007/2007report.htm. The website is http://untreaty.un.org/ilc/summaries/7_6.htm (last visited 10 March 2010) (last visited March 2010).

[11] See Report of the International Law Commission, Sixty-first session (May-August 2009), General Assembly Official Reports, Sixty-fourth session, Supplement No. 10, A/64/10 at http://untreaty.un.org/ilc/reports/2009/2009report.htm, especially chapter 9 at http://untreaty.un.org/ilc/reports/2009/english/chp9.pdf, and Third Report of 10 June 2008 from Special Rapporteur, A/CN.4/603 at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/375/23/PDF/N0837523.pdf?OpenElement (last visited 10 March 2010). See also, Amnesty Document - International Law Commission: The obligation to extradite or prosecute (aut dedere aut judicare)(Amnesty 2009) at http://www.amnesty.org/en/library/asset/IOR40/001/2009/en/a16af900-f20a-11dd-855f-392123cb5f06/ior400012009en.html (last visited 10 March 2010).

[12] See pages 8-10 in Criminal Justice Assessment Toolkit: Cross-Cutting Issues # 4 - International Cooperation (UNODC, 2006) at http://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/4_International_Cooperation.pdf (last visited 10 March 2010).

[13] See pages 8-10 in Criminal Justice Assessment Toolkit: Cross-Cutting Issues # 4 - International Cooperation (UNODC, 2006) at http://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/4_International_Cooperation.pdf (last visited 10 March 2010).

[14] As acts or incidents may suddenly appear to be everywhere and at the same time for anyone, any court or any State might argue that it has jurisdiction. This approach I have labeled with the term "*Global Jurisdiction*," which is characterized by a State's jurisdictional rules being taken on its "wording" to reach all alien cybernauts, thus conferring jurisdiction involving aliens outside the forum state anywhere in the world . The term needs to be distinguished from Universal Jurisdiction. HENRIK SPANG-HANSSEN, PUBLIC INTERNATIONAL COMPUTER NETWORK LAW ISSUES page v, Foreword (DJØF Publishing, 2006); Henrik Spang-Hanssen , *The Future of International Law: CyberCrime* at section 3.1 (2007)(available from the Social Science Research Network's (SSRN's) Working Paper Series at http://ssrn.com/abstract=1090876).

compared or confused with "Universal Jurisdiction"[15] – and basically have attempted to indict any computer user on earth if the particular country's criminal laws embraced the act as a violation.[16]

Such a state of affairs is clearly an unreasonable regime, given that it requires any individual user of the Internet to know the laws of all of the sovereign states on the planet.

Consequently, we need a truly international Internet Crime Convention that prevents Internet users from being indicted in foreign countries for violations they were "rightfully" unaware of.

Now, there are, of course, situations in which cybernauts can be well aware that their acts via computer will have effects in foreign countries (consider the example Enrico above).

But in other cases cybernauts will have no idea their use of a computer has foreign implications (as in the example above of Louise uploading her article). Even if she were well aware of her own national constitution/law, she would presumably have no idea of the law existing on a different continent. In most cases the adults bringing up Louise, that is her parents and educators, would have no such knowledge either – and would be most surprised that her act was illegal and that she could potentially be extradited for it.

So there must be new rules of public international law governing cyberspace and the limits of national jurisdiction over Cyberspace, including that:

- What a cybernaut does on the Internet is most likely an international case – thus, not subject to domestic law alone,. And also, thus, that a national court cannot ignore international and foreign law.
- Public international law must resolve the question of where "the place" of the criminal act is.[17]
- Let it be stated by the international society that what is done legally in the cybernaut's own country shall not cause such individual to be charged or indicted in a foreign country or countries – except for cases of extreme harm that are reasonably foreseeable.

Next, the international community must decide on the rest of the Standards and Norms for Cyberspace issues. For example, to what extent – if any – should "spamming" be considered a (cyber-)crime?[18] The percentage of electronic spam is often similar to the percentage of unsolicited mail in a physical mailbox. Thus, spam could be held to be a "service-provider problem" (that is, not having enough copper wire/broadband for PR-commercials) rather than regarded as a crime similar to a distribution of service attack ("DoS") (that is, making a computer resource unavailable to its intended users by intentionally overwhelming it with data – "a network terrorist-attack").

As for acts that are not destructive of computer networks – that is, pure information on the Internet – a lesson could be learned from developers of the IP (Internet Protocol), who stated: "Be liberal in what you accept, and conservative in what you send" and who also suggested that we "teach our children to think more deeply about what they see and hear" because "[t]hat, more than any electronic filter [and laws], will build a foundation upon which truth can stand."

Then – and only then – will it be possible to decide what should be a cybercrime and how to prevent it – through education of computer users and others associated with the Internet.

A commentary to the so-called "Stanford Proposal" remarks, that "Cyber crime is quintessentially transnational, and will often involve jurisdictional assertions of multiple states. To

---

[15] "*Universal Jurisdiction*" is allowed in certain instances by the international community, and a court of a nation acts on behalf of the international community pursuant to public international law. "*Universal Jurisdiction*" can only be exercised when the international community has accepted it – and if so it will only be for a very limited and specific issue -- for example, war crimes or piracy. HENRIK SPANG-HANSSEN, CYBERSPACE & INTERNATIONAL LAW ON JURISDICTION 252-254 (DJØF Publishing, 2004), IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 303 (6th Ed., Clarendon Press), OPPENHEIM'S INTERNATIONAL LAW 469-470 (9th Ed., Longman).

[16] However, "Global Jurisdiction" (see my definition above in footnote 14) is prohibited by public international law, which requires closeness (a close link) and reasonableness between the jurisdiction and the alien in question. Furthermore, under public international law any jurisdiction has to respect the sovereignty of other States and their right to self-determination of rules for and over their citizens.

[17] A separate paper of mine will deal with this vital issue for Cyberspace.

[18] Cybercrime Offences Under National Law usually deal with: A. Have illegal access to computer data and systems, illegal interception, data interference, and system interference been criminalized? B. Have computer-related forgery and fraud been criminalized? C. Have the necessary substantive and procedural laws to prevent and punish terrorist and other criminal activities perpetuated with the aid of computers and computer networks been enacted? Section 3.1.9, page 7 in Criminal Justice Assessment Toolkit: Cross-Cutting Issues # 4 - International Cooperation (UNODC, 2006) at http://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/4_International_Cooperation.pdf (last visited 10 March 2010).

avoid the conflict such assertions of jurisdiction could cause, enforcement under the Stanford Draft is limited to cyber activities that are universally condemned. The Stanford Draft does not accede to a state's jurisdiction merely because someone within its territory is able to access a website in another state; to confer jurisdiction, someone in control of the website must deliberately cause one of the covered crimes, with effects in the state seeking to assert jurisdiction. It seems likely, therefore, that states will in general accept all of the reasonably based jurisdictional claims approved in the Draft."[19]

Thus, the "Stanford Proposal" – which recognized cyber crime is essentially transnational and thus involves jurisdictional assertions of multiple states – tries to avoid this conflict by limiting its scope to cyber activities that are universally condemned.

This would safeguard protection of the individual cybernaut and "regain" the cybernaut's fundamental human rights.

The flipside of the coin, however, is that such limitation on extradition does not imply there should not be cooperation on a larger scale between states on investigation and enforcement.

Thus, the international community really should conclude another international treaty dealing with cooperation between states on investigations of cybercrime – similar to the CyberCrime Convention's articles 25-35 on cooperation between States.

4. Final Remarks

We need a truly international Internet Crime Convention that prevents Internet users from being indicted in foreign countries for criminal violations of which they cannot reasonably be held to be aware.

I sincerely hope this Congress will consider asking the UN Commission on Crime and Criminal Justice to draft and prepare for the next Congress an Internet Crime Convention related to crimes where a computer has been used, which:

- integrates UN Crime Prevention and Criminal Justice Standards and Norms
- suggests how best to provide international education and training on the use of Cyberspace – without risk of charge/indictment anywhere on the planet.
- deals with protection[20] of the individual cybernaut from criminalization of his/her acts by foreign states and resulting extradition – except in cases where the international community has expressly condemned particular (universal) acts.

[19] Abraham D. Sofaer, Toward an International Convention on Cyber Security in reprinted in THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 233 (A. Sofaer and S. Goodman, eds., Hoover Institution Press 2001 – ISBN 0-8179-9982-5). Also available from http://www.hoover.org/publications/books/cybercrime.html (last visited 9 March 2010).

[20] Incorporating but not limited to the scope of: African Charter on Human and Peoples' Rights 1986; African Charter on the Rights and Welfare of the Child 1990; Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms 1953; American Convention on Human Rights 1969; (OAS) American Declaration of the Rights and Duties of Man, O.A.S. Res. XXX [AG/RES. 1591 (XXVIII-O/98)], adopted by the Ninth International Conference of American States, Bogotá, Colombia (1948); European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment 1989. Annex A, page 31 in Criminal Justice Assessment Toolkit: Cross-Cutting Issues # 2 - Juvenile Justice (UNODC, 2006) at http://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/2_Juvenile_Justice.pdf (last visited 10 March 2010).

APPENDIX 1: Article 7 of (Stanford) Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (Extradition)[21]

1. Offenses under the domestic laws of each State Party concerning any conduct set forth in Articles 3 and 4 shall be deemed to be included as extraditable offenses in any extradition treaty existing between or among States Parties. States Parties undertake to include such offenses as extraditable offenses in every extradition treaty subsequently concluded between them; however, failure to include these offenses in such treaties shall not affect the obligations undertaken herein.

2. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention as the legal basis for extradition in respect of the offenses covering conduct set forth in Articles 3 and 4. Extradition shall remain subject to any other requirement of the law of the requested State.

3. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offenses covering the conduct set forth in Articles 3 and 4 as extraditable offenses as between themselves, subject to any other requirement of the law of the requested State.

4. Offenses covering the conduct set forth under Articles 3 and 4 shall to that extent be treated, for the purpose of extradition between States Parties, as if they had been committed in the place in which they occurred, and also in the territories of the State or States required or authorized to establish their jurisdiction under Article 5.

5. When extradition is requested by more than one requesting State Party, the requested State Party shall respond to such requests in accordance with the priorities for jurisdiction set out in Article 5, paragraph 4.

[21] See http://media.hoover.org/documents/0817999825_249.pdf (last visited 9 March 2010).

APPENDIX 2: Article 24 of CyberCrime Convention of 2001[22] (Extradition)

1. a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition,[23] applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7. a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.
b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

---

[22] See http://conventions.coe.int/treaty/en/treaties/html/185.htm (last visited 9 March 2010).
[23] European Convention on Extradition of 13. December 1957 (entered into force 18 April 1960), ETS No. 24 at http://conventions.coe.int/Treaty/en/Treaties/Html/024.htm (47 ratifications as of 13 April 2007).